Welcome to the PIA for FY 2010!

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

Directions:

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program. More information can be found by reading VA 6508.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: http://vaww.privacy.va.gov/PIA.asp

Roles and Responsibilities:

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the Privacy Impact Assessment Handbook 6202.2 referenced in the procedure section of this document.

a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Handbook 6202.2.

b. Records Officer is responsible for supplying records retention and deletion schedules.

c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Handbook 6202.2 and to immediately report all anomalies to the Privacy Service and appropriate management chain.

d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.

e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and

systems, coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues, and reviewing and approving the PIA before submission to the Privacy Service.

Definition of PII (Personally Identifiable Information)

Information in identifiable form that is collected and stored in the system that either directly identifies and individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect indentify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

Macros Must Be Enabled on This Form

To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

(FY 2010) PIA: System Identification

Program or System Name:	FPO>VHA>HRC>LAN (Local Area Network)
OMB Unique System / Application / Program Identifier (AKA: UPID #):	029-00-02-00-01-1120-00
Description of System / Application / Program:	The Local Area Network (LAN) system is a general support system comprised of workstations, thin clients, servers, printers and Cisco network switches. The LAN system also includes subsystem components such as tape drives, disk drives, uninterruptible power supplies (UPS), and storage access networks (SAN). The workstations and severs operate in an Windows environment. The HRC LAN is part of the greater VA wide interconnected network.

Facility Name: Health Resource Center (HRC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Tracey Sugihara	785-350-3746	Tracey.Sugihara@va.gov
Information Security Officer:	Kevin R Jones	785-350-1809	Kevin.Jones1@va.gov
Chief Information Officer:	Thomas Puckett	785-350-1802	Thomas.Puckett@va.gov
Person Completing Document:	Kevin R Jones	785-350-1809	
Other Titles:			

Other Titles:
Other Titles:

Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)	07/2008
Date Approval To Operate Expires:	08/2011

What specific legal authorities authorize this program or system:	Title V USC 301, Title 38* USC 501	
What is the expected number of individuals that will have their PII stored in this system:	Approximately 3 million	*Note: The HRC LAN has a subsystem or major applicatin called CRM or OSCR. This application is the repository for all information collected from calls received. CRM (OSCR) is also tracked in SMART and has it's own PIA, SSP, and related documents. This number and most refernces to sensitive data are actually referring to the CRM subsystem.
Identify what stage the System / Application / Program is at:	Operations/Maintenance	
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.	13 years	
Is there an authorized change control process which documents any changes to existing applications or systems?	Yes	
If No, please explain:		
Has a PIA been completed within the last three years?	Yes	

Date of Report (MM/YYYY): 07/2008

Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.

- ☐ Have any changes been made to the system since the last PIA?
- ☐ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☑ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☑ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☑ Does this system/application/program collect, store or disseminate the SSN?

If there is no Personally Identifiable Information on your system , please skip to TAB 12. (See Comment for Definition of PII)

(FY 2010) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records?	Yes
if the answer above is no, please skip to row 16.	
For each applicable System(s) of Records, list:	
1. All System of Record Identifier(s) (number):	02VA135
2. Name of the System of Records:	Applications for Employement under Title 38, Records - VA
3. Location where the specific applicable System of Records Notice may be accessed (include the URL):	All SORNS can be accessed at: http://www.va.gov/privacy/systemsofrecords/
Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
	(Please Select Yes/No)
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	No
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	No
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes

Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

18VA05
Centralized Staffing System - VA

*Privacy office sends written notification to all Veterans registered with the VA. This is a National Common Control.

(FY 2010) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Family Relation (spouse, children, parents, grandparents, etc)	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Service Information	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Medical Information	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Criminal Record Information	ALL	The HRC only collects Criminal record information for employees as part of their employment application and HR records.	Written	Written
Guardian Information	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Education Information	ALL	The HRC only collects educational information on employees as part of their employment application and HR records.	Written	Written
Benefit Information	ALL	The caller is asked to validate information for identity verification.	Verbally	Written
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Voluntary	Used to Validate identity
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	Used to validate the right to talk about the veteran or primary subject.
Service Information	Yes	Veteran	Voluntary	Used to help determine services available and validate records.
Medical Information	Yes	VA Files / Databases (Identify file)	Voluntary	Used to open case records to manage veteran's case.
Criminal Record Information	Yes	Veteran	Voluntary	Asked on aplications and background checks to determine employment suitability.
Guardian Information	Yes	Veteran	Voluntary	Contact information on veteran and guardian to validate access to veterans records and to establish case records.
Education Information	Yes	Veteran	Voluntary	Collected during application for employment process used to determine suitability for employment

Benefit Information	Yes	VA Files / Databases (Identify file)	Voluntary	
Other (Explain)				This category is open ended, it depends on what infor mation the veteran or primary subjects is requesting for/or informs call agent for case record
Other (Explain)	Yes	Veteran	Voluntary	
Other (Explain)				

(FY 2010) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Department of Veteran's Affairs	Yes	Other VA Facilities Access CIRTS and CRM/PRM for case resolution. They have access to all data contained.	Both PII & PHI	Annual Privacy Training. Only VA employees access HRC LAN resources
Other Veteran Organization		No			
Other Federal Government Agency		No			
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System					
Other Project / System					
Other Project / System					

(FY 2010) PIA: Access to Records

Does the system gather information from another system?	Yes	
Please enter the name of the system:	VA VistA systems	
Per responses in Tab 4, does the system gather information from an individual?	Yes	
If information is gathered from an individual, is the information provided:	☐ Through a Written Request ☐ Submitted in Person ☐ Online via Electronic Form	* N/A - The HRC is a Call Center for Veterans. The only means for information to be provided from an individual is verbally over the telephone. The facility is closed to the public and does not do any direct patient care.

Is there a contingency plan in place to process information when the system is down?	Yes

(FY 2010) PIA: Secondary Use

Will PII data be included with any secondary use request?	No
if yes, please check all that apply:	☐ Drug/Alcohol Counseling ☐ Mental Health ☐ HIV ☐ Research ☐ Sickle Cell ☐ Other (Please Explain)
Describe process for authorizing access to this data. Answer:	

(FY 2010) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public? If Yes, Please Specify:	No
Explain how collected data are limited to required elements: Answer:	Quality Assurance (QA) team and supervisors reviews. Electronic validation checks.
How is data checked for completeness? Answer:	QA team and supervisors reviews. Electronic validation checks.
What steps or procedures are taken to ensure the data remains current and not out of date? Answer:	CCPC data refreshed daily from AAC databases. Otherwise relevant data is validated with each call.
How is new data verified for relevance, authenticity and accuracy? Answer:	CCPC is used for electronical validatation. Each time a customer calls in, relevant data is checked against CCPC.
Additional Information: (Provide any necessary clarifying information or additional explanation for this section.) Answer:	

(FY 2010) PIA: Retention & Disposal

What is the data retention period? Answer:	CCPC – 120 days of billing statements. CRM - 6 months after case resolved. CoNexus – no less than 18 months.
Explain why the information is needed for the indicated retention period? Answer:	Information is retained to work cases and in case of congressional inquiry.
What are the procedures for eliminating data at the end of the retention period? Answer:	Electronically (Scheduled scripts and processes are run to purge it)
Where are these procedures documented? Answer:	In the System design specifications.
How are data retention procedures enforced? Answer:	Electronically.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)	Yes

Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)

Answer:

(FY 2010) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13? No

If Yes, How will parental or guardian approval be obtained?

Answer:

(FY 2010) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	Yes
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls..	Yes
Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information?	Yes
If 'No' to any of the 3 questions above, please describe why: Answer:	
Is adequate physical security in place to protect against unauthorized access? If 'No' please describe why: Answer:	Yes
Explain how the project meets IT security requirements and procedures required by federal law. Answer:	The HRC follows national VA and NIST guidance. Multiple systems such as SMART and REMEDY are used as Central points of management for the entire VA. Please see the System Security Plan.

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- [x] Air Conditioning Failure
- [x] Chemical/Biological Contamination
- [ ] Blackmail
- [x] Bomb Threats
- [x] Cold/Frost/Snow
- [x] Communications Loss
- [x] Computer Intrusion
- [x] Data Destruction
- [x] Data Disclosure
- [x] Data Integrity Loss
- [x] Denial of Service Attacks
- [x] Earthquakes
- [x] Eavesdropping/Interception
- [x] Fire (False Alarm, Major, and Minor)
- [x] Flooding/Water Damage
- [x] Hardware Failure
- [x] Malicious Code
- [x] Computer Misuse
- [x] Power Loss
- [x] Sabotage/Terrorism
- [x] Storms/Hurricanes
- [ ] Substance Abuse
- [x] Theft of Assets
- [x] Theft of Data
- [x] Vandalism/Rioting
- [x] Errors (Configuration and Data Entry)
- [x] Burglary/Break In/Robbery
- [ ] Identity Theft
- [ ] Fraud/Embezzlement

Answer: (Other Risks)

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- [x] Risk Management
- [x] Access Control
- [x] Awareness and Training
- [x] Contingency Planning
- [x] Physical and Environmental Protection
- [x] Personnel Security
- [x] Certification and Accreditation Security Assessments
- [x] Audit and Accountability
- [x] Configuration Management
- [x] Identification and Authentication
- [x] Incident Response
- [x] Media Protection

Answer: (Other Controls) All Security Controls are documented in the SSP.

PIA: PIA Assessment

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: No Change, the system is in Operations/Maintenance phase.

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☐	The potential impact is HIGH if the loss of Availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑	The potential impact is MODERATE if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is LOW if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? **(Choose One)**	☑	The potential impact is high if the loss of Integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☐	The potential impact is moderate if the loss of Integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is LOW if the loss of Integrity could be expected to have a limited adverse effect on operations, assets or individuals.
Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? **(Choose One)**	☐	The potential impact is high if the loss of Confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	☑	The potential impact is moderate if the loss of Confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	☐	The potential impact is LOW if the loss of Confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Please add additional controls:

(FY 2010) PIA: Additional Comments

Add any additional comments on this tab for any question in the form you want to comment on.
Please indicate the question you are responding to and then add your comments.

(FY 2010) PIA: VBA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

Records Locator System
Veterans Assistance Discharge System (VADS)
LGY Processing
Loan Service and Claims
LGY Home Loans
Search Participant Profile (SPP)
Control of Veterans Records (COVERS)
SHARE
Modern Awards Process Development (MAP-D)
Rating Board Automation 2000 (RBA2000)
State of Case/Supplemental (SOC/SSOC)
Awards
Financial and Accounting System (FAS)
Eligibility Verification Report (EVR)
Automated Medical Information System (AMIS)290
Web Automated Reference Material System (WARMS)
Automated Standardized Performace Elements Nationwide (ASPEN)
Inquiry Routing Information System (IRIS)
National Silent Monitoring (NSM)
Web Service Medical Records (WebSMR)
Systematic Technical Accuracy Review (STAR)
Fiduciary STAR Case Review
Veterans Exam Request Info System (VERIS)
Web Automated Folder Processing System (WAFPS)
Courseware Delivery System (CDS)
Electronic Performance Support System (EPSS)
Veterans Service Representative (VSR) Advisor
Loan Guaranty Training Website
C&P Training Website

Education Training Website
VR&E Training Website
VA Reserve Educational Assistance Program
Web Automated Verification of Enrollment
Right Now Web
VA Online Certification of Enrollment (VA-ONCE
Automated Folder Processing System (AFPS)
Personal Computer Generated Letters (PCGL)
Personnel Information Exchange System (PIES)
Rating Board Automation 2000 (RBA2000)
SHARE
State Benefits Reference System
Training and Performance Support System (TPSS)
Veterans Appeals Control and Locator System (VACOLS)
Veterans On-Line Applications (VONAPP)
Automated Medical Information Exchange II (AIME II)
Committee on Waivers and Compromises (COWC)
Common Security User Manager (CSUM)
Compensation and Pension (C&P) Record Interchange (CAPRI)
Control of Veterans Records (COVERS)
Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
Fiduciary Beneficiary System (FBS)
Hearing Officer Letters and Reports System (HOLAR)
Inforce
Awards
Actuarial
Insurance Self Service
Insurance Unclaimed Liabilities
Insurance Online

Appraisal System
Web Electronic Lender Identification
CONDO PUD Builder
Centralized Property Tracking System
Electronic Appraisal System
Web LGY
Access Manager
SAHSHA
VBA Data Warehouse
Distribution of Operational Resources (DOOR)
Enterprise Wireless Messaging System (Blackberry)
VBA Enterprise Messaging System
LGY Centralized Fax System
Review of Quality (ROQ)
Automated Sales Reporting (ASR)
Electronic Card System (ECS)
Electronic Payroll Deduction (EPD)
Financial Management Information System (FMI)
Purchase Order Management System (POMS)
Veterans Canteen Web
Inventory Management System (IMS)
Synquest
RAI/MDS
ASSISTS
MUSE
Bbraun (CP Hemo)
VIC
BCMA Contingency Machines
Script Pro

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments
			Is PII collected by this minor application?	
Minor app #1			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
			Is PII collected by this minor application?	
Minor app #2			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
			Is PII collected by this minor application?	
Minor app #3			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

Baker System

Dental Records Manager

Sidexis

Priv Plus

Mental Health Asisstant

Telecare Record Manager

Omnicell

Powerscribe Dictation System

EndoSoft

Compensation and Pension (C&P)

Montgomery GI Bill

Vocational Rehabilitation & Employment (VR&E) CH 31

Post Vietnam Era educational Program (VEAP) CH 32

Spinal Bifida Program Ch 18

C&P Payment System

Survivors and Dependents Education Assistance CH 35

Reinstatement Entitelment Program for Survivors (REAPS)

Educational Assistance for Members of the Selected Reserve Program CH 1606

Reserve Educational Assistance Program CH 1607

Compensation & Pension Training Website

Web-Enabled Approval Management System (WEAMS)

FOCAS

Work Study Management System (WSMS)

Benefits Delivery Network (BDN)

Personnel and Accounting Integrated Data and Fee Basis (PAID)

Personnel Information Exchange System (PIES)

Rating Board Automation 2000 (RBA2000)

SHARE

Service Member Records Tracking System

Veterans Assistance Discharge System (VADS)

VBA Training Academy

Veterans Service Network (VETSNET)

Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)

BIRLS

Centralized Accounts Receivable System (CARS)

Compensation & Pension (C&P)

Corporate Database

Control of Veterans Records (COVERS)

Data Warehouse

INS - BIRLS

Mobilization

Master Veterans Record (MVR

BDN Payment History

(FY 2010) PIA: VISTA Minor Applications

Explain what minor application that are associated with your installation? *(Check all that apply)*

ACCOUNTS RECEIVABLE	DRUG ACCOUNTABILITY	INPATIENT MEDICATIONS
ADP PLANNING (PLANMAN)	DSS EXTRACTS	INTAKE/OUTPUT
ADVERSE REACTION TRACKING	EDUCATION TRACKING	INTEGRATED BILLING
ASISTS	EEO COMPLAINT TRACKING	INTEGRATED PATIENT FUNDS
AUTHORIZATION/SUBSCRIPTION	ELECTRONIC SIGNATURE	INTERIM MANAGEMENT SUPPORT
AUTO REPLENISHMENT/WARD STOCK	ENGINEERING	KERNEL
AUTOMATED INFO COLLECTION SYS	ENROLLMENT APPLICATION SYSTEM	KIDS
AUTOMATED LAB INSTRUMENTS	EQUIPMENT/TURN-IN REQUEST	LAB SERVICE
AUTOMATED MED INFO EXCHANGE	EVENT CAPTURE	LETTERMAN
BAR CODE MED ADMIN	EVENT DRIVEN REPORTING	LEXICON UTILITY
BED CONTROL	EXTENSIBLE EDITOR	LIBRARY
BENEFICIARY TRAVEL	EXTERNAL PEER REVIEW	LIST MANAGER
CAPACITY MANAGEMENT - RUM	FEE BASIS	MAILMAN
CAPRI	FUNCTIONAL INDEPENDENCE	MASTER PATIENT INDEX VISTA
CAPACITY MANAGEMENT TOOLS	GEN. MED. REC. - GENERATOR	MCCR NATIONAL DATABASE
CARE MANAGEMENT	GEN. MED. REC. - I/O	MEDICINE
CLINICAL CASE REGISTRIES	GEN. MED. REC. - VITALS	MENTAL HEALTH
CLINICAL INFO RESOURCE NETWORK	GENERIC CODE SHEET	MICOM
CLINICAL MONITORING SYSTEM	GRECC	MINIMAL PATIENT DATASET
CLINICAL PROCEDURES	HEALTH DATA & INFORMATICS	MYHEALTHEVET
CLINICAL REMINDERS	HEALTH LEVEL SEVEN	Missing Patient Reg (Original) A4EL
CMOP	HEALTH SUMMARY	NATIONAL DRUG FILE
CONSULT/REQUEST TRACKING	HINQ	NATIONAL LABORATORY TEST
CONTROLLED SUBSTANCES	HOSPITAL BASED HOME CARE	NDBI
CPT/HCPCS CODES	ICR - IMMUNOLOGY CASE REGISTRY	NETWORK HEALTH EXCHANGE
CREDENTIALS TRACKING	IFCAP	NOIS
DENTAL	IMAGING	NURSING SERVICE
DIETETICS	INCIDENT REPORTING	OCCURRENCE SCREEN
DISCHARGE SUMMARY	INCOME VERIFICATION MATCH	ONCOLOGY
DRG GROUPER	INCOMPLETE RECORDS TRACKING	ORDER ENTRY/RESULTS REPORTING

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

	Name		Description	Comments
Minor app #1				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #2				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

	Name		Description	Comments
Minor app #3				
			Is PII collected by this min or application?	
			Does this minor application store PII?	
			If yes, where?	
			Who has access to this data?	

OUTPATIENT PHARMACY

PAID
PATCH MODULE
PATIENT DATA EXCHANGE

PATIENT FEEDBACK

PATIENT REPRESENTATIVE

PCE PATIENT CARE ENCOUNTER
PCE PATIENT/IHS SUBSET

PHARMACY BENEFITS MANAGEMENT
PHARMACY DATA MANAGEMENT
PHARMACY NATIONAL DATABASE
PHARMACY PRESCRIPTION PRACTICE
POLICE & SECURITY

PROBLEM LIST

PROGRESS NOTES

PROSTHETICS
QUALITY ASSURANCE INTEGRATION
QUALITY IMPROVEMENT CHECKLIST
QUASAR

RADIOLOGY/NUCLEAR MEDICINE
RECORD TRACKING

REGISTRATION

RELEASE OF INFORMATION - DSSI

REMOTE ORDER/ENTRY SYSTEM
RPC BROKER

RUN TIME LIBRARY
SAGG
SCHEDULING

SECURITY SUITE UTILITY PACK

SHIFT CHANGE HANDOFF TOOL

SOCIAL WORK

SPINAL CORD DYSFUNCTION
SURGERY
SURVEY GENERATOR

TEXT INTEGRATION UTILITIES

TOOLKIT

UNWINDER

UTILIZATION MANAGEMENT ROLLUP

UTILIZATION REVIEW

VA CERTIFIED COMPONENTS - DSSI

VA FILEMAN

VBECS

VDEF

VENDOR - DOCUMENT STORAGE SYS

VHS&RA ADP TRACKING SYSTEM

VISIT TRACKING
VISTALINK

VISTALINK SECURITY

VISUAL IMPAIRMENT SERVICE TEAM ANRV
VOLUNTARY TIMEKEEPING

VOLUNTARY TIMEKEEPING NATIONAL

WOMEN'S HEALTH

CARE TRACKER

(FY 2010) PIA: Minor Applications

Add any information concerning minor applications that may be associated with your system. Please indicate the name of the minor application, a brief description, and any comments you may wish to include. If you have more than 3 minor applications please copy then below sections as many times as needed.

	Name		Description		Comments
Minor app #1					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #2					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

	Name		Description		Comments
Minor app #3					
			Is PII collected by this min or application?		
			Does this minor application store PII?		
			If yes, where?		
			Who has access to this data?		

(FY 2010) PIA: Final Signatures

Facility Name: Health Resource Center (HRC)

Title:	Name:	Phone:	Email:
Privacy Officer:	Tracey Sugihara	785-350-3746	Tracey.Sugihara@va.gov
SUGIHARA, TRACEY, HRC — Digital Signature Block	Digitally signed by: SUGIHARA, TRACEY, HRC DN: CN = SUGIHARA, TRACEY, HRC O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.12 15:59:25 -06'00' Reason: I am approving this document		
Information Security Officer:	Kevin R Jones	785-350-1809	Kevin.Jones1@va.gov
Kevin R. Jones — Digital Signature Block	Digitally signed by: KEVIN JONES DN: CN = KEVIN JONES O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.12 14:49:40 -06'00'		
Chief Information Officer:	Thomas Puckett	785-350-1802	Thomas.Puckett@va.gov
THOMAS PUCKETT — Digital Signature Block	Digitally signed by: THOMAS PUCKETT DN: CN = THOMAS PUCKETT O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.12 16:11:59 -06'00'		
Person Completing Document:	Kevin R Jones	785-350-1809	0
Kevin R. Jones — Digital Signature Block	Digitally signed by: KEVIN JONES DN: CN = KEVIN JONES O = Department of Veterans Affairs OU = Dept. of Veterans Affairs, Internal Staff Date: 2010.01.12 14:49:16 -06'00'		
System / Application / Program Manager:	0	0	0
Digital Signature Block			

Date of Report:	1/12/2010
OMB Unique Project Identifier	029-00-02-00-01-1120-00
Project Name	FPO>VHA>HRC>LAN (Local Area Network)